REMARKS

I. General

Claims 1-15 were pending in the application, and all of such claims were rejected in the present Office Action mailed April 3, 2006. The issues raised in the present Office Action are:

- Claims 1-15 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,279,113 issued to Vaidya (hereinafter "*Vaidya*").

In response, Applicant respectfully traverses the outstanding claim rejections, and requests reconsideration and withdrawal thereof in light of the remarks presented herein. No amendments to claims 1-15 are presented herein. New claims 16-20 are presented herein. Claims 16-20 do not add any new matter, as they are fully supported by the specification.

II. Rejections Under 35 U.S.C. §102 over *Vaidya*

Under 35 U.S.C. §102, a claim is anticipated only if each and every element as set forth in the claim is found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987); M.P.E.P. §2131. In addition, "[t]he identical invention must be shown in as complete detail as is contained in the ... claims" and "[t]he elements must be arranged as required by the claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. §2131. Applicant respectfully traverses the rejection of claims 1-15 because *Vaidya* fails to teach all elements of the claims as discussed below.

Independent Claim 1

Independent claim 1 recites, in part, "a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system implemented as an intermediate driver and bound to the protocol driver and the media access control driver" (emphasis added). *Vaidya* fails to teach at least this element of claim 1. The present Office Action asserts that column 7, lines 18-24 of *Vaidya* teaches this element, *see* page 7 of the Office Action. Column 7, lines 11-24 of *Vaidya* provides:

> With reference to FIG. 4, the operation of the virtual processor 36 includes monitoring network data 46 to determine whether the data is associated with a network intrusion. A register cache 40 temporarily stores information extracted from a data packet which determines which signature profile(s) will be accessed from the signature profile memory 39. The virtual processor 36 obtains a data packet from a queue and extracts MAC header information, IP header information, transport header information, and application information from the data packet. Extraction of the packet information enables the data collector 10 to detect network intrusions based in the different layers of the OSI model.

The above portion of *Vaidya* fails to teach an instance of an intrusion prevention system that is implemented as an intermediate driver that is bound to a protocol driver and a media access control driver. While the above portion of *Vaidya* mentions that certain MAC header information, IP header information, transport header information, and application information is extracted from a received data packet, *Vaidya* makes no mention of implementing an intrusion prevention system as an intermediate driver that is bound to a protocol driver and a media access control driver within a network stack. The above portion of *Vaidya* appears to suggest that the monitoring of the 7 layers of the OSI model is limited to pulling a data packet from a queue and then extracting data from the data packet for analysis. By contrast, claim 1 recites that intrusion protection is implemented as part of "a network stack [of an operating system]" and, specifically, implemented as "an intermediate driver" of the network stack. *Vaidya* simply provides no express or inherent teaching (either in the above-quoted portion or elsewhere) of such an implementation, and therefore *Vaidya* fails to anticipate claim 1.

In view of the above, Applicant respectfully requests that the rejection of claim 1 be withdrawn. Each of dependent claims 2-5 depend from claim 1, and thus inherit all limitations of claim 1. It is respectfully submitted that dependent claims 2-5 are allowable at least because of their dependency from claim 1 for the reasons discussed above.

Independent Claim 13

Independent claim 13 recites, in part, "determining a correspondence between the packet and at least two of the plurality of machine-readable network-exploit signatures" (emphasis added). The present Office Action asserts that reference number 64 in figure 3 of *Vaidya*, along with column 7, lines 12-24 of *Vaidya* teach this element. Applicant disagrees.

Column 7, lines 11-24 of *Vaidya* provides:

> With reference to FIG. 4, the operation of the virtual processor 36 includes monitoring network data 46 to determine whether the data is associated with a network intrusion. A register cache 40 temporarily stores information extracted from a data packet which determines which signature profile(s) will be accessed from the signature profile memory 39. The virtual processor 36 obtains a data packet from a queue and extracts MAC header information, IP header information, transport header information, and application information from the data packet. Extraction of the packet information enables the data collector 10 to detect network intrusions based in the different layers of the OSI model.

The above portion of *Vaidya* fails to teach determining a correspondence between a packet and at least two machine-readable network-exploit signatures. The above teaching of *Vaidya* provides that data is extracted from a data packet and used to determine which signature profile(s) will be accessed. Nothing in *Vaidya* teaches a scenario in which a correspondence between a packet and at least two machine-readable network-exploit signatures is determined. While one or more signature profiles may be accessed, nothing in *Vaidya* teaches that at least two signatures can be determined as having correspondence with a packet. *Vaidya* explains at column 3, lines 27-48:

> The attack signature profiles are organized into sets of attack signature profiles which are assigned to network objects based on security requirements of the network objects, and these sets of signature profiles are stored in a signature profiles memory. The signature profile memory of a network defines the network data signaling patterns which constitute network intrusion attempts with regard to that network. Association data is stored in the signature profile memory and corresponds each of the network objects to associated set or subset of signature profiles, such that multiple sets of signature profiles are assigned to the set of network objects.
>
> Data transmitted over the network is monitored by a data monitoring device to detect data addressed to the network objects. Upon detecting data addressed to one of the network objects, a set of signature profiles corresponding to that network object is accessed from the signature profile memory based on the association data. At least one attack signature profile from the set of profiles is processed by the processor to determine if the data addressed to the network object is associated with a network intrusion.

While *Vaidya* mentions that multiple signature profiles may be accessed to determine if the packet is associated with a network intrusion, nothing in *Vaidya* teaches that a plurality of signatures can be determined as corresponding to a packet. For instance, if a signature contained in a first profile of *Vaidya* corresponds to a packet, the actions associated with such

signature may be taken; but nothing in *Vaidya* teaches that in such a case further analysis may be performed to determine whether another signature (e.g., of a second profile) also corresponds to the packet. Rather, in accessing the profiles of *Vaidya*, it appears that once a first signature is determined to correspond to the packet, an associated network intrusion may be detected, without further proceeding to also determine whether other signatures may correspond to the packet. Certainly *Vaidya* fails to provide teaching "in as complete detail as is contained in" claim 1 of determining correspondence between a packet and at least two machine-readable network-exploit signatures, and therefore fails to anticipate claim 1, *see Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. §2131.

In view of the above, Applicant respectfully requests that the rejection of claim 13 be withdrawn. Each of dependent claims 14-15 and newly added claims 16-20 depend from claim 13, and thus inherit all limitations of claim 13. It is respectfully submitted that dependent claims 14-20 are allowable at least because of their dependency from claim 13 for the reasons discussed above.

III. Conclusion

In view of the above, Applicant believes the pending application is in condition for allowance.

Applicant believes no fee is due with this response. However, if a fee is due, please charge Deposit Account No. 80-2025, under Order No. 10017333-1 from which the undersigned is authorized to draw.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV 568242715US in an envelope addressed to: MS Amendment, Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: June 29, 2006

Typed Name: Gail Miller

Signature: Gail Miller

Respectfully submitted,

By: _____

Jody C. Bishop
Attorney/Agent for Applicant(s)
Reg. No. 44,034
Date: June 29, 2006
Telephone No. (214) 855-8007